Office of the Governor
State Chief Information Officer

SECURITY

Chapter 10 – Addressing Personnel Issues Relating to Security

Scope: These policies apply to all public agencies, their agents or designees subject to Article 3D of Chapter 147, "State Information Technology Services."

Statutory Authority: N.C.G.S. §147-33.110

Section 01 Contractual Documentation

100101 Preparing Terms and Conditions of Employment

The above standard recommended by ISO 17799 is addressed in Chapter 126 – State Personnel Act and in policies established by the Office of State Personnel.

100102 Employing/Contracting New Staff

The standard recommended by ISO 17799 for this category is addressed in Chapter 11 of this document, "Delivering Training and Staff Awareness."

100103 Contracting with External Suppliers/Other Service Providers

Purpose: To address information security issues involving third parties who provide services to State agencies.

STANDARD

Each agency shall ensure that third parties who provide information technology services agree to follow the agency's information technology security policies when providing services to the agency.

Third parties are non-State employees, such as vendors, suppliers, individuals, contractors and consultants, responsible for providing goods or services to the State. In order to perform the requested services, a third party might need to use agency information technology assets and access agency information determined to be valuable to operations and/or classified as non-public or restricted by law. Access must be granted to third-party users only when required for performing work and with the full knowledge and prior approval of the information asset owner. Third parties shall be fully accountable to the State for any actions taken while completing their agency assignments. Agency staff overseeing the work of third parties shall be responsible for communicating and enforcing applicable laws, as well as State and agency security policies, and procedures.

ISO 17799: 2005 References
6.1.3 Allocation of Information Security responsibilities

100104 Using Non Disclosure Agreements (Third Party)

Purpose: To protect access to and the integrity of the State's information resources.

STANDARD

State agency operational and/or restricted information must not be released to third parties without properly executed contracts and confidentiality agreements. These legal documents, which may include non-disclosure agreements, must specify conditions of use and security requirements.

ISO 17799: 2005 References
6.1.5 Confidentiality agreements

100105 Misuse of Organization Stationery
100106 Lending Keys to Secure Areas to Others
100107 Lending Money to Work Colleagues

If appropriate, the above policies recommended by ISO 17799 should be addressed by the agency personnel office or senior management.

100108 Complying with Information Security

Purpose: To reduce employee violations of an agency's information technology security policies.

STANDARD

Agencies shall require their employees with access to the State Network to comply with the more stringent of statewide and agency-specific information technology security policies and standards.

ISO 17799: 2005 References
8.1.1 Roles and responsibilities
8.2.3 Disciplinary process
15.2.1 Compliance with security policies and standards

100109 Establishing Ownership of Intellectual Property Rights

The standard recommended by ISO 17799 in this category is not appropriate as an information technology security standard for North Carolina executive branch agencies.

ISO 17799: 2005 References
8.1.1 Roles and responsibilities
15.1.1 Identification of applicable legislation

100110 Employees' Responsibility to Protect Confidentiality of Data

Purpose: To protect the confidentiality of confidential records maintained by State government.

STANDARD

The standard recommended by ISO 17799 in this category is not appropriate as an information technology security standard for North Carolina executive branch agencies.

GUIDELINES

Agencies should consider requiring their employees who have access to confidential data to sign nondisclosure agreements.

ISO 17799 References
8.1.1 Roles and responsibilities
15.1.4 Data protection and privacy of personal information

Section 02 Confidential Personnel Data

100201 Respecting Privacy in the Workplace

The standard recommended by ISO 17799 in this category is addressed in Standard 020109, Monitoring System Access and Use.

100202 Handling Confidential Employee Information

The standard recommended by ISO 17799 in this category is governed by N.C.G.S. Chapter 126 – State Personnel Act.

100203 Giving References on Staff

The standard recommended by ISO 17799 in this category is governed by agency personnel practices.

100204 Checking Staff Security Clearance

The standard recommended by ISO 17799 in this category is governed by N.C.G.S. Chapter 126 – State Personnel Act.

100205 Sharing Employee Information with Other Employees

The standard recommended by ISO 17799 in this category is governed by N.C.G.S. Chapter 126 – State Personnel Act.

100206 Sharing Personal Salary Information

The standard recommended by ISO 17799 in this category is governed by N.C.G.S. Chapter 126 – State Personnel Act.

Section 03 Personnel Information Security Responsibilities

100301 Using the Internet in an Acceptable Way

Purpose: To establish a standard pertaining to the use of the State Network and the global Internet by state employees and other state network users.

STANDARD

While performing work-related functions, while on the job, or while using publicly owned or publicly provided information processing resources, state employees and other state network users shall be expected to use the State Network and the Internet responsibly and professionally and shall make no intentional use of these services in an illegal, malicious or obscene manner.

Each agency shall determine the extent of personal use its employees and other State Network users may make of the State Network and the Internet.

All files downloaded from a source external to the State Network shall be scanned for viruses, Trojan horses, worms or other destructive code for such harmful contents. This includes files obtained as email attachments and through any other file transfer mechanism. It shall be the responsibility of public employees and State Network users to help prevent the introduction or propagation of computer viruses. All agencies shall ensure that they have current software on their networks to prevent the introduction or propagation of computer viruses.

State employees and other state network users shall not access or attempt to gain access to any computer account which they are not authorized to access. They shall not access or attempt to access any portions of the State Network to which they are not authorized to have access. Public employees and other State Network users also shall not intercept or attempt to intercept data transmissions of any kind that they are not authorized to have access.

Operators of email services must create an abuse@<*host domain name*> account and other additional internal procedures to manage their email complaints. Users who receive email that they consider to be unacceptable according to this standard can choose to forward the original email message (including all headers) to the appropriate email abuse@<*host domain name*> account.

GUIDELINES

Agencies may want to address other acceptable use issues in their own internal policies on subjects such as use of instant messaging, and personal use of state computers.

ISO 17799 References
8.2.3 Disciplinary process
15.1.5 Prevention of misuse of information processing facilities

100302 Keeping Passwords/PIN Numbers Confidential

Purpose: To reduce unauthorized access to information technology systems

STANDARD

Except as specifically allowed by the security administrator, passwords shall not be revealed to anyone, including supervisors, family members or coworkers. In

special cases where a user must divulge a password, such as for system support, the user shall immediately change the password after the purpose for revealing the password has been achieved.

ISO 17799 References
8.2.3 Disciplinary process
15.1.5 Prevention of misuse of information processing facilities

100303 Sharing Confidential Organization Information with Other Employees

The standard recommended by ISO 17799 for this category is addressed in Standard 020110, Giving Access to Files and Documents.

100304 Using E-mail and Postal Mail Facilities for Personal Use

The standard recommended by ISO 17799 for this category with regard to email is addressed in Standard 100301, Using the Internet in an Acceptable Way. The remainder of the recommended standard is more appropriately addressed by the Office of State Personnel and agency management.

100305 Using Telephone Systems for Personal Reasons
100306 Using the Organization's Mobile Phones for Personal Use
100307 Using Organization Credit Cards
100308 Signing for Delivery of Goods
100309 Signing for Work Done by Third Parties
100310 Ordering Goods and Services
100311 Verifying Financial Claims and Invoices
100312 Approving and Authorization of Expenditures

The above standards recommended by ISO 17799 should be addressed by the appropriate management of each agency, if appropriate.

100313 Responding to Telephone Inquiries

The standard recommended by ISO 17799 for this category is addressed in Standard 030406, Giving Instructions over the Telephone.

100314 Sharing Confidential Information with Family Members
100315 Gossiping and Disclosing Information
100316 Spreading Information through the Office "Grape Vine"

The standards recommended by ISO 17799 in the above three categories are governed by State and federal laws for confidential records, and agencies should address the issues through their personnel policies, if appropriate.

100317 Playing Games on Office Computers

The standard recommended by ISO 17799 in this category should be addressed by individual agency policies, if appropriate.

100318 Using Office Computers for Personal Use

The standard recommended by ISO 17799 for this category is addressed in Standard 100301, Using the Internet in an Acceptable Way.

Section 04 – HR Management

The policies recommended by ISO 17799 in this section are more appropriately addressed by the Office of State Personnel and individual agency personnel managers.

Section 05 – Staff Leaving Employment

The policies recommended by ISO 17799 in this section are more appropriately addressed by the Office of State Personnel and individual agency personnel managers.

Section 06 – HR Issues Other

The standard recommended by ISO 17799 in this section is more appropriately addressed by the Office of State Personnel and individual agency personnel managers.

HISTORY

State CIO Approval:
Original Issue Date:
Subsequent History:

Standard Number	Version	Date	Change/Description

Old Security Policy/Standard	New Standard Numbers
Use of the North Carolina State Network and the Internet	**100301** Using the Internet in an Acceptable Way